

REMARKS

Applicants appreciate the Examiner's thorough examination of the subject application and request reconsideration of the subject application based on the foregoing amendments and the following remarks.

Claims 1-6 and 8-22 are pending in the subject application.

Claim 7 was previously canceled.

Claims 1-6 and 8-22 stand rejected under 35 U.S.C. §103.

Claim 14 and 16 were canceled in the instant amendment without prejudice to prosecuting them in a continuing application.

Claims 1, 17 and 18 were amended to more distinctly claim embodiments of Applicants' invention.

Claims 3, 13, and 19-22 were amended to reflect changes in the language of the related base claim and/or any intervening claims.

The amendments to the claims are supported by the originally filed disclosure.

35 U.S.C. §103 REJECTIONS

Claims 1-6 and 8-22 stand rejected under 35 U.S.C. §103 as being unpatentable over the cited prior art for the reasons provided on pages 2-9 of the above-referenced Office Action. Applicants respectfully traverse as discussed below.

Because claims 14 and 16 were cancelled in the foregoing amendment, Applicants have not addressed the within rejections further herein as to these claims. Because claims were amended in the instant amendment, the following discussion refers to the language of the amended claims. However, only those amended features specifically relied upon to distinguish the claimed invention from the cited prior art shall be considered as being made to overcome the

cited reference. The following addresses the specific rejections provided in the above-referenced Office Action.

CLAIMS 1-6, 8-14 & 17-22

Claims 1-6, 8-14 and 17-22 stand rejected as being unpatentable over Dimotroff [USP 6,212,606] in view of “Windows 2000 Quick Fixes(“Boyce”) for the reasons provided on pages 2-8 of the above referenced Office Action. Applicants respectfully traverse.

As indicated above, as claim 14 was cancelled in the foregoing amendment, Applicants have not addressed the within rejection further herein as to claim 14.

In claim 1, Applicants claim an electronic device network system that includes an electronic device for transmitting print data via a network; plurality of storing means for storing the print data transmitted from the electronic device; a plurality of printers for acquiring the print data from the storing means and printing the acquired print data; a setting section; a network connecting the electronic device, the plurality of storing means, and the plurality of printers to one another; a search means; and a selecting means. Such a setting section sets a security level of the print data to be transmitted, where the security level of the print data is set in the setting section responsive to an input from a user of the electronic device. The set security level is selected by the user is selected from a plurality of identified security levels of the print data.

The electronic device, at least one of the plurality of storing means, and at least one of the plurality of printers each have a security function and another security level associated with the set security level of the print data. At least one of the plurality of storing means has a security level that is different from another of the plurality of storing means, and at least one of the plurality of printers has a security level that is different from another of the plurality of printers.

The search means searches the plurality of storing means and searches the plurality of printers, responsive to selection of the security level of the print data by the user, so as to identify

one or more given storing means and one or more given printers each of whose security level corresponds to the security level of the print data which security level is set in the setting section.

The selecting means provides the results of the searching to the user and provides an output. The output corresponds to: (i) a selected one of the identified one or more given storing means whose security level corresponds to the security level of the print data which security level is set in the setting section and (ii) a selected one of the identified one or more given printers whose security level corresponds to the security level of the print data which security level is set in the setting section, where the selected ones being selected by the user from the provided search results.

The electronic device transmits the print data to the selected one of the given storing means in response to the output from the selecting means. The transmitted print data is transmitted to the selected one of the given printers by the selected one of the given storing means.

In other words, for the electronic network device of claim 1: (1) a security level is set from a plurality of such security levels for the print data to be transmitted; (2) a search is made to identify those storing means and printers whose security level corresponds to the security level set in the setting section for the print data, (3) the results of the searching are provided to the user who selects one of the storing means and printers were identified in (2); and (4) after the user selects, the electronic network device transmits the print data to the selected storing means which also transmits the print data to the selected printer. Thus, the electronic device of claim 1 is configured and arranged so that the user provides inputs at different times which inputs are utilized to control the electronic network device. In this way, the user can send the print data to a particular storage means/device and printer that have a desired security level for the print data.

As can be seen from the following discussion, Dimitroff does not describe, teach or suggest an electronic device network system as set forth in claim 1. More particularly, Dimitroff does not describe, teach or suggest “a search means for searching the plurality of storing means and for searching the plurality of printers, responsive to selection of the security level of the print

data by the user, so as to identify one or more given storing means and one or more given printers each of whose security level corresponds to the security level of the print data which security level is set in the setting section.” Moreover, the discussion in Dimitroff does not describe, teach or suggest setting a security level for searching which set security level relates to the security level of the print data.

In contrast to the electronic device network system of claim 1, Dimitroff describes and teaches a computer system 100 that is preferably configured using a system network 102 such as a Local Area Network (LAN), a System Area Network (SAN) or a Wide Area Network (WAN). The system network 102 can be a high-speed communication system designed to link several workstations 104 and hosts 106 (e.g., servers/initiators) together so as to share computing resources including hardware, application programs and information. The hosts 106 connect to a storage area network 108 (e.g., peer network/storage topology) using line 110, where the storage area network is transport independent.

It also is described in Dimitroff that the storage area network 108 also connects to at least one controller 112 or at least one intelligent controller 114 using lines 116. Each controller 112 or intelligent controller 114 is coupled with or incorporated into a corresponding storage unit 118 that operates to store data including files and images. In addition, each controller 112 and intelligent controller 114 may be capable of writing, reading and reformatting data from and to any of the hosts 106 or respective storage units 118.

As further described in Dimitroff, one aspect of Dimitroff’s invention includes classifying the different capabilities of storage units 118 by establishing different standardized shared levels (e.g., first shared level 212, second shared level 214, third shared level 216 and fourth shared level 218) based on the specific parametrics or physical properties of the particular storage unit 118. The different types of storage units 118 (e.g., optical drive 128 and tape drive 120) can still have the same parametrics or shared levels 212, 214, 216, or 218. Dimitroff further provides that the parametrics can be classified into a security parametric 240 (optional), an access parametric 250, an availability parametric 260, an ownership parametric 270 and a management parametric

280. Each of these parametrics 240, 250, 260 and 270 can be further divided into multiple levels. Again, the various parametrics 240, 250, 260, and 270 are used to classify and identify the physical properties and capabilities of each storage unit 118.

In the discussion regarding the first shared level, Dimitroff also provides that *the lack of the security parametric 240* indicates that any one of the hosts 106 can have ownership of the storage unit 118.

The presence of the ownership parametric 270 typically indicates that one of the hosts 106 can be associated with a particular storage unit 118 and controller 112 or 114. More specifically, the ownership parametric 270 includes a first ownership level 272 that requires the storage unit 118 to respond with a busy signal to all other hosts while communicating with one of the hosts 106. The first ownership level 272 may also be referred to as "Command Ownership". The storage unit 118 can be available but functionally inaccessible due to the status of the first ownership level 272.

In the discussion regarding the fourth shared level Dimitroff describes the security parametric 240 in more detail because the fourth level includes a security parametric/security level. In regards to the fourth shared level Dimitroff provides, that any storage unit 118 (*e.g.*, disk drive sub-system 126 and optical drive subsystem 130) assigned the fourth shared level 218 includes the parametrics of one security level 242 from the security parametric 240, three access levels 252, 254, and 256 from the access parametric 250, one availability level 262 from the availability parametric 262, three ownership levels 272, 274 and 276 from the ownership parametric 270 and three management levels 282, 284 and 286 from the management parametric 280. Again, the hosts 106 or user are able to identify a shareability characteristic of a particular storage unit 118 by referring to the corresponding standardized shared level 212, 214, 216 or 218.

It is further provided in Dimitroff, that the fourth shared level 218 may not be limited to the first security level 242 in the storage unit 118, but it also can include selected ones of a second security level 244, a third security level 246 and a fourth security level 248. As further described in Dimitroff, the second security level 244 requires the hosts 106 to use a password

before gaining access to the storage unit; the third security level 246 requires the hosts to use either an encrypted password or an encrypted data password before gaining access to the storage unit 118 and before gaining access to data located on the storage unit, respectively and the fourth security level 248 requires the hosts 106 to use both the encrypted password and the encrypted data password.

In other words, the discussion in Dimitroff regarding the different security levels in connection with the fourth shared level, describes the different mechanisms or protocols the user or host must comply with in order to gain access to a particular storage unit. It should be remembered that the host/user must already have ownership rights to begin with in order for the user/host to even attempt to comply with any security criterion being imposed by the security level.

In sum, and as indicated above, Dimitroff does not describe, teach or suggest “a search means for searching the plurality of storing means and for searching the plurality of printers, responsive to selection of the security level of the print data by the user, so as to identify one or more given storing means and one or more given printers each of whose security level corresponds to the security level of the print data which security level is set in the setting section.” This should not be surprising as a search of the patent’s text for Dimitroff does not show that the word “printer” was used anywhere in this patent.

Moreover, the discussion in Dimitroff does not describe, teach or suggest setting a security level for searching which set security level relates to the security level of the print data. Rather Dimitroff describes establishing different security protocols to gain access to a storage unit where the host/user must have pre-established ownerships rights to such a storage unit.

Based on the limited use of Boyce in connection with the present grounds for rejection and in view of Applicants’ prior remarks regarding Boyce, Applicants respectfully submit that that Boyce does not overcome the above described shortcomings for Dimitroff.

There also is no suggestion, description or teaching in either Dimitroff or Boyce, alone or in combination, that would suggest or teach that if the system in Dimitroff was revised or altered so as to yield the electronic device network system of claim 1, that such a system would be reasonably successful.

As to claims 2-6 and 8-13, each of these claims depends (directly or ultimately) from claim 1. Thus, each of claims 2-6 and 8-13 are considered to be allowable at least because of their dependency from an allowable base claim. This shall not, however, be considered an admission that claims 2-6 and 8-13 are not separately patentable from the identified combination of references.

As to claim 17, Applicants respectfully submit that the above remarks regarding claim 1, apply to distinguish the data receiver search system of claim 17 from the identified combination of references. This shall not, however, be considered an admission that there are not additional grounds for distinguishing claim 17 from the identified combination of references.

As to claim 18, Applicants respectfully submit that the above remarks regarding claim 1 apply to distinguish the data receiver search method of claim 18 from the identified combination of references. This shall not, however, be considered an admission that there are not additional grounds for distinguishing claim 18 from the identified combination of references.

As to claims 19-22, each of these claims depends (directly or ultimately) from claim 18. Thus, each of claims 19-22 are considered to be allowable at least because of their dependency from an allowable base claim. This shall not, however, be considered an admission that claims 19-22 are not separately patentable from the identified combination of references.

It is respectfully submitted that claims 1-6, 8-13 and 17-22 are patentable over the cited reference(s) for the foregoing reasons.

CLAIMS 15 - 16

Claims 15 and 16 stand rejected as being unpatentable over Dimotroff in view of Boyce and further in view of Tomat [USP 6,459,499] for the reasons provided on pages 2-8 of the above referenced Office Action. Applicants respectfully traverse.

As indicated above, as claim 16 was cancelled in the foregoing amendment, Applicants have not addressed the within rejection further herein as to claim 16.

As to claim 15, this claim depends from claim 1. Thus, claim 15 is considered to be allowable at least because of its dependency from an allowable base claim. This shall not be considered an admission that claim 15 is not otherwise patentable over the identified combination of references.

It is respectfully submitted that claim 15 is patentable over the cited reference(s) for the foregoing reasons.

The following additional remarks shall apply to each of the above.

A prior art reference can be combined or modified to reject claims as obvious as long as there is a reasonable expectation of success. *In re Merck & Co., Inc.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Additionally, it also has been held that if the proposed modification or combination would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. Further, the teaching or suggestion to make the claimed combination and the reasonable suggestion of success must both be found in the prior art, not in applicant's disclosure. *In re Vaack*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). As can be seen from the foregoing discussion regarding the disclosures of the cited references and the admitted prior art, there is no reasonable expectation of success provided in the reference or the admitted prior art. Also, it is clear from the foregoing discussion that the modification suggested by the Examiner would change the principle of operation of the device disclosed in the reference.

Applicant: Naoki Asada et al.
U.S.S.N.: 10/767,878
Response to Non-Final Office Action
Page 19 of 19

It is respectfully submitted that for the foregoing reasons, claim(s) 1-6 and 8-13, 15, and 17-22 are patentable over the cited reference(s) and satisfy the requirements of 35 U.S.C. §103. Therefore, these claims are allowable.

It is respectfully submitted that the subject application is in a condition for allowance. Early and favorable action is requested.

Applicants believe that additional fees are not required for consideration of the within Response. However, if for any reason a fee is required, a fee paid is inadequate or credit is owed for any excess fee paid, the Commissioner is hereby authorized and requested to charge Deposit Account No. **04-1105**.

Respectfully submitted,
Edwards Angell Palmer & Dodge, LLP

/ William J. Daley, Jr. /

Date: October 7, 2009

By: _____
William J. Daley, Jr.
(Reg. No. 35,487)
P.O. Box 55874
Boston, MA 02205
(617) 239-0100

Customer No. 21,874

Bos2_759392